



Notfallzettel: Handy weg

Verloren, gestohlen, beschlagnahmt · gehört zu Kapitel 5 und 17 · Gerät: _____ · Stand der Vorsorge: _____

Erst die Konten, dann das Gerät. Ein gestohlenes GrapheneOS-Gerät mit starkem Passwort und automatischem Neustart ist für den Dieb ein Ziegelstein: Nach dem Neustart liegen keine Schlüssel mehr im Arbeitsspeicher, der Speicher bleibt vollständig verschlüsselt, und Fehlversuche beim Entsperren bremsen das Sicherheitselement bis zum Stillstand aus, nach zwanzig Fehlversuchen ist Schluss. Das eigentliche Risiko ist nicht das Gerät, sondern alles, was daran hängt: die SIM, die Codes empfängt, das E-Mail-Konto, mit dem sich Passwörter zurücksetzen lassen, die Zwei-Faktor-Token, die Bank. Dieser Zettel sortiert den Ernstfall so, dass die Konten zuerst drankommen. Er trägt aber nur, wenn die obere Hälfte vorher erledigt ist.

A · VORHER, DAMIT DER ZETTEL IM ERNSTFALL TRÄGT

Punkt	OK	Notiz
Die Sicherung läuft regelmäßig und wurde einmal probeweise zurückgespielt. Sie ist verschlüsselt, bevor sie das Gerät verlässt, das Ziel darf also auch ein fremder Speicher sein (Kapitel 5).		Rhythmus: _____
Der Wiederherstellungscod e liegt auf Papier an einem Ort, den du im Ernstfall erreichst. Ohne ihn ist die Sicherung wertlos. Hier nur das Kürzel des Ortes eintragen.		Liegt bei: _____
Der Zwei-Faktor-Tresor (Aegis) hat ein Backup außerhalb des Geräts, aktualisiert nach jedem neuen Token, etwa auf einem getrennt aufbewahrten USB-Stick und in einer verschlüsselten Cloud. Vault-Passwort und Backup-Passwort sind unabhängig davon gesichert, im Passwort-Manager und auf Papier (Kapitel 17).		Backup bei: _____
Der Passwort-Manager ist von einem zweiten Gerät aus erreichbar. Master-Passwort im Kopf, Anmeldung auf dem Rechner oder Zweitgerät einmal geprobt. Sonst fehlt im Ernstfall der Schlüssel zu allem anderen.		
IMEI und Kaufbeleg liegen zu Hause. Die IMEI ist die Gerätekennung, die an der Hardware hängt und mit keinem SIM-Wechsel verschwindet (Kapitel 6). Polizei und Anbieter fragen danach.		Liegt bei: _____
Anbieter-Hotline für die SIM-Sperre notiert (unten im Feld). Die SIM ist in Deutschland, Österreich und der Schweiz an deine Identität gebunden, also auch an deine Verträge und Kosten.		
Ein zweites Gerät oder ein Rechner steht für den Notfall bereit, mit dem du Konten erreichst und ein Ersatzgerät einrichten kannst.		Steht bei: _____
Automatischer Neustart und ein starkes Passwort sind aktiv. Das ist der eigentliche Diebstahlschutz: kein Dienst in der Ferne, sondern ein Gerät, das ohne dich nichts preisgibt (Kapitel 5).		Intervall: _____

B · IM ERNSTFALL, IN DIESER REIHENFOLGE

Nr	Schritt	Warum	Erledigt
1	SIM sperren lassen. Anbieter anrufen, Nummer sperren, Ersatz-SIM oder eSIM-Profil bestellen.	Keine SMS-Codes und Anrufe an fremde Hand, keine fremden Kosten auf deinem Vertrag.	
2	Passwort-Manager und Haupt-E-Mail sichern , von einem anderen Gerät aus: Passwort ändern, alle Sitzungen abmelden, Wiederherstellungswege prüfen.	Über die Haupt-E-Mail lassen sich fast alle anderen Passwörter zurücksetzen. Sie ist der Generalschlüssel.	
3	Messenger: Gerät aus den Konten abmelden, wo möglich, sonst neu registrieren und Kontakte informieren. Nostr-Schlüssel gilt bei einer reinen Handy-Kopie als gefährdet.	Sonst liest oder schreibt ein Fremder in deinem Namen weiter.	
4	Bank und Zahlungsdienste informieren , Karten und Banking-Apps sperren, Freigabeverfahren auf dem Ersatzgerät neu einrichten.	Freigabe-Apps und Karten in der Wallet sind Geld in fremder Hand, sobald ein Konto fällt.	
5	Zwei-Faktor aus dem Aegis-Backup auf dem Ersatzgerät wiederherstellen. Dafür brauchst du Backup-Datei und Backup-Passwort.	Ohne Token sperrst du dich sonst selbst aus den Konten aus, die du gerade schützt.	
6	Bitcoin: Schlüssel auf der Hardware-Wallet (BitBox02) sind nicht betroffen, sie haben das Gerät nie verlassen. Eine reine Handy-Wallet gilt als gefährdet: Guthaben von einem sauberen Gerät aus auf eine neue Wallet mit neuem Seed bewegen.	Ein Angreifer, der das Passwort doch knackt, hätte sonst Zeit auf seiner Seite.	
7	Anzeige mit IMEI erstatten , Anbieter über den Diebstahl informieren, Vorgangsnummer notieren.	Anzeige und IMEI braucht es für Versicherung, Anbieter und den Fall, dass das Gerät auftaucht.	
8	Neues Gerät aus der Sicherung wiederherstellen , mit dem Wiederherstellungscod vom Papier. Danach die Punkte aus Teil A erneut abhaken.	Die Sicherung ist der einzige Weg zurück zu deinen Daten. Der Code ist der einzige Schlüssel dazu.	
9	Falls das Gerät zurückkommt: als kompromittiert behandeln. Nicht weiter benutzen, GrapheneOS neu installieren, aus der Sicherung wiederherstellen (Kapitel 19).	Manipulation ist in kurzer Zeit möglich und nicht ohne Weiteres erkennbar.	

Anbieter-Hotline: _____ · Bank-Sperrnummer: _____ · Zweites Gerät steht bei (Kürzel): _____ · Wer wird informiert: _____

⚠ Kein Fernorten, kein Fernlöschen. GrapheneOS bringt keinen Google-Dienst zum Orten oder Löschen aus der Ferne mit und verzichtet laut FAQ bewusst auf die Rücksetz-Sperre, weil sie Diebstahlabschreckung ist und keine Sicherheitsfunktion. Ein Dieb kann das Gerät also zurücksetzen und weiterverwenden. An deine Daten kommt er dabei nicht, wenn Passwort und automatischer Neustart aktiv sind. Die Vorsorge aus Teil A ersetzt beides. **⚠ Keine Passwörter, PINs oder Wiederherstellungscodes auf diesen Zettel.** Er darf gefunden werden, ohne dass er etwas verrät. Orte nur als Kürzel.